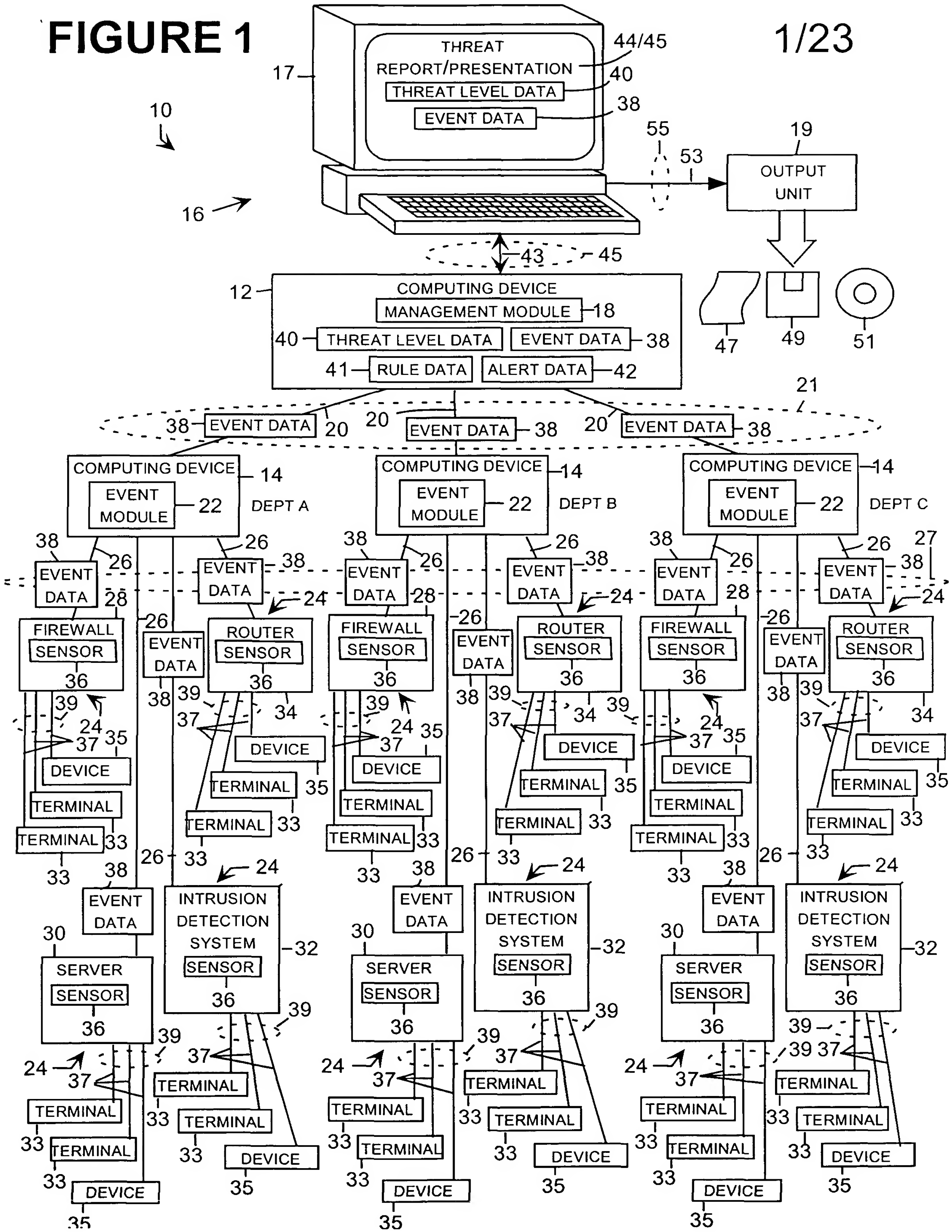
FIGURE 1


10
16
17
THREAT REPORT/PRESENTATION
44/45
THREAT LEVEL DATA
40
EVENT DATA
38
55
53
19
OUTPUT UNIT
47
49
51
43
45
12
COMPUTING DEVICE
MANAGEMENT MODULE
18
40
THREAT LEVEL DATA
EVENT DATA
38
41
RULE DATA
ALERT DATA
42
21
20
EVENT DATA
38
COMPUTING DEVICE
14
EVENT MODULE
22
DEPT A
DEPT B
DEPT C
26
28
27
24
FIREWALL
ROUTER
SENSOR
36
39
37
34
35
DEVICE
TERMINAL
33
INTRUSION DETECTION SYSTEM
32
SERVER
30

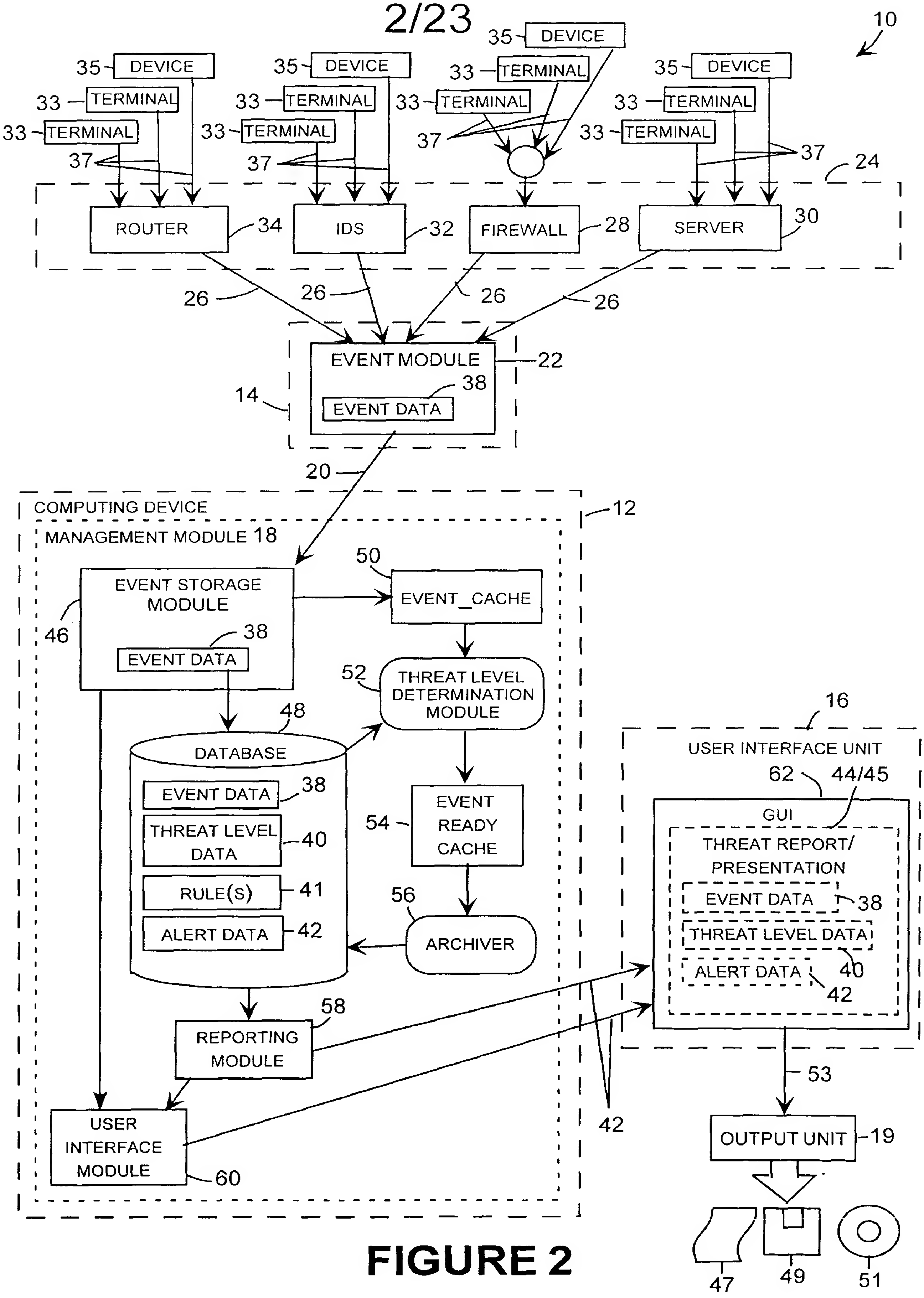

10
35 DEVICE
33 TERMINAL
33 TERMINAL
37
35 DEVICE
33 TERMINAL
33 TERMINAL
37
35 DEVICE
33 TERMINAL
33 TERMINAL
37
35 DEVICE
33 TERMINAL
33 TERMINAL
37
24
ROUTER 34
IDS 32
FIREWALL 28
SERVER 30
26
26
26
26
EVENT MODULE 22
38
EVENT DATA
14
20
COMPUTING DEVICE
12
MANAGEMENT MODULE 18
EVENT STORAGE MODULE
46
38
EVENT DATA
50
EVENT_CACHE
52
THREAT LEVEL DETERMINATION MODULE
48
DATABASE
EVENT DATA 38
THREAT LEVEL DATA 40
RULE(S) 41
ALERT DATA 42
54
EVENT READY CACHE
56
ARCHIVER
58
REPORTING MODULE
USER INTERFACE MODULE
60
42
16
USER INTERFACE UNIT
62
44/45
GUI
THREAT REPORT/ PRESENTATION
EVENT DATA 38
THREAT LEVEL DATA 40
ALERT DATA 42
53
OUTPUT UNIT 19
47
49
51

FIGURE 2

SINGLE MANAGEMENT MODULE AND
MULTIPLE EVENT MODULES

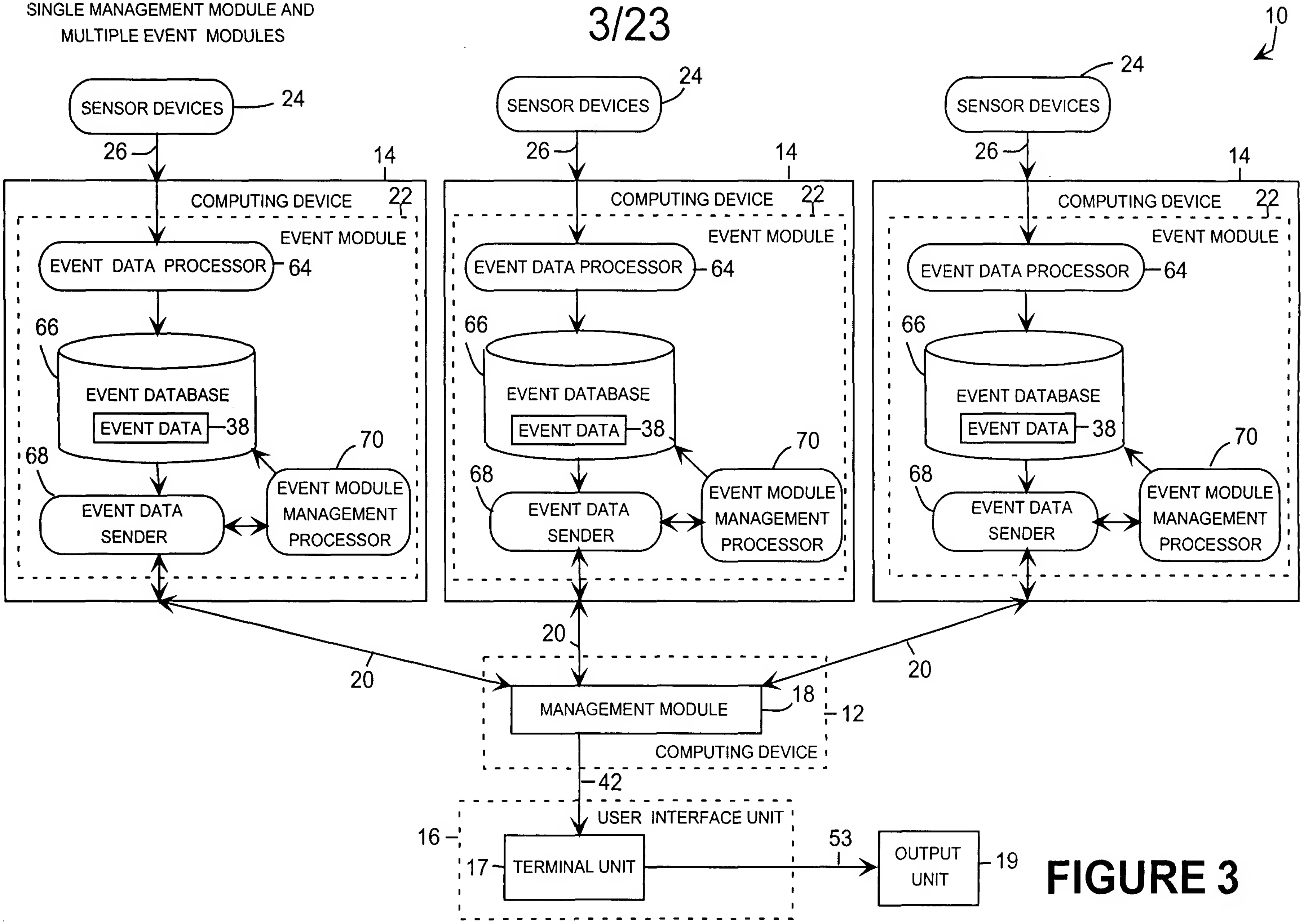


FIGURE 3

SINGLE MANAGEMENT MODULE AND
REDUNDANT EVENT MODULES

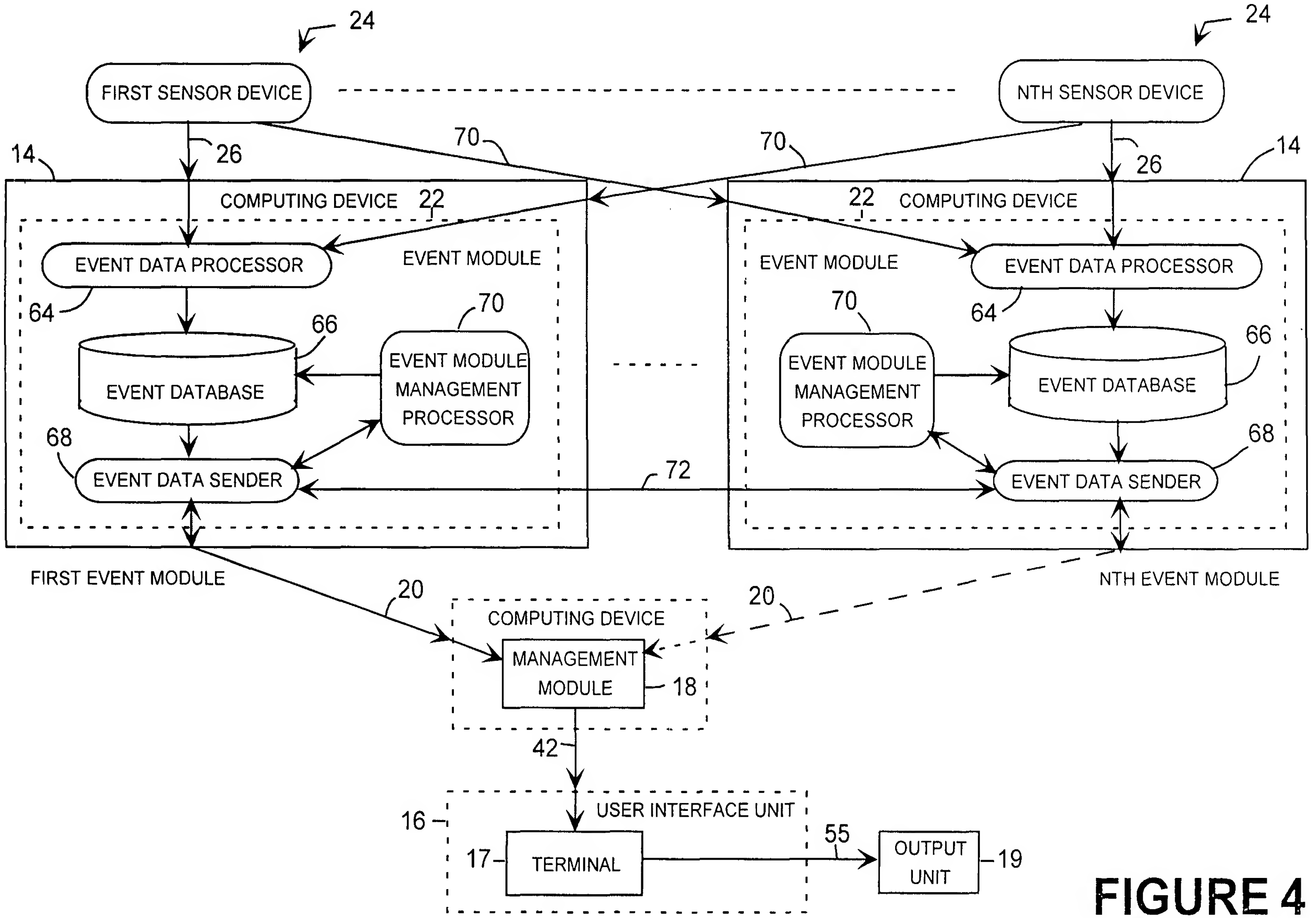


FIGURE 4

FIGURE 5

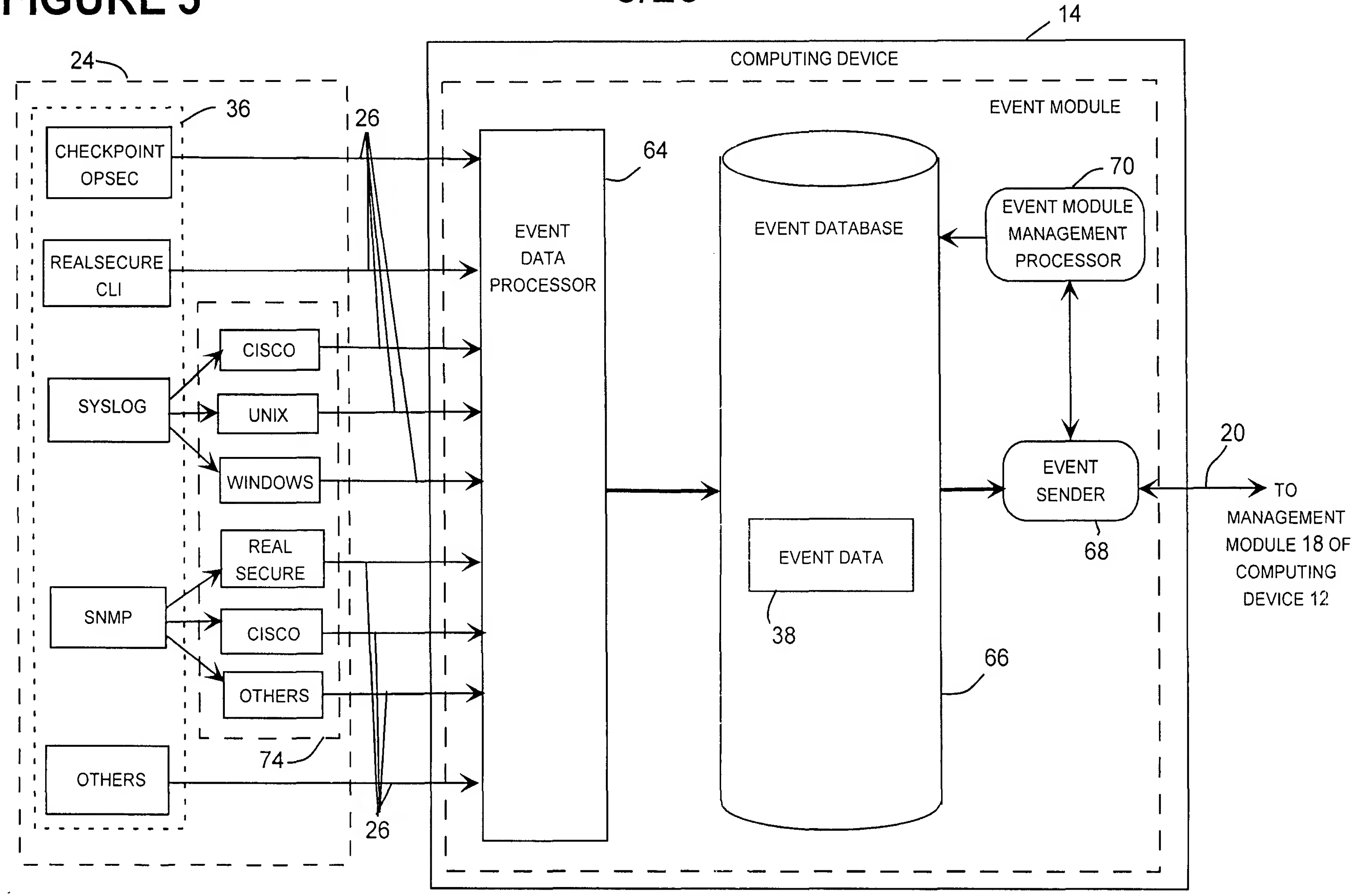

24
36
26
CHECKPOINT OPSEC
REALSECURE CLI
SYSLOG
SNMP
OTHERS
CISCO
UNIX
WINDOWS
REAL SECURE
CISCO
OTHERS
74
26
14
COMPUTING DEVICE
EVENT MODULE
EVENT DATA PROCESSOR
64
EVENT DATABASE
EVENT DATA
38
66
70
EVENT MODULE MANAGEMENT PROCESSOR
EVENT SENDER
68
20
TO MANAGEMENT MODULE 18 OF COMPUTING DEVICE 12

FIGURE 6

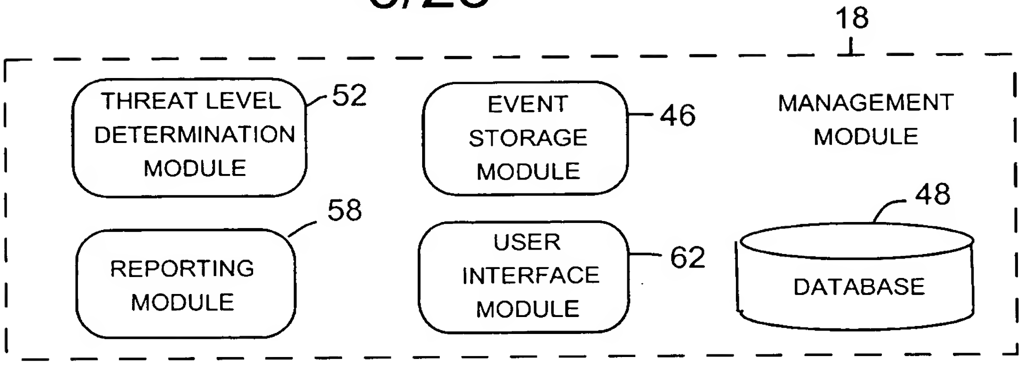


FIGURE 7

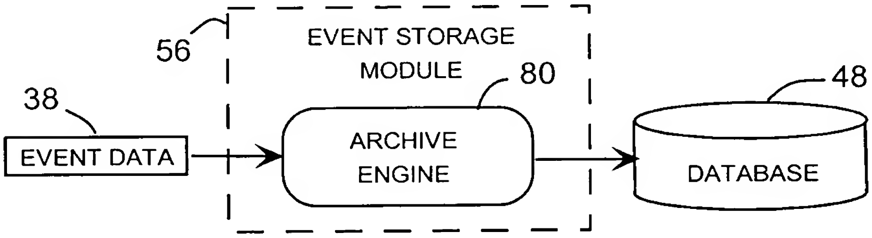


FIGURE 8

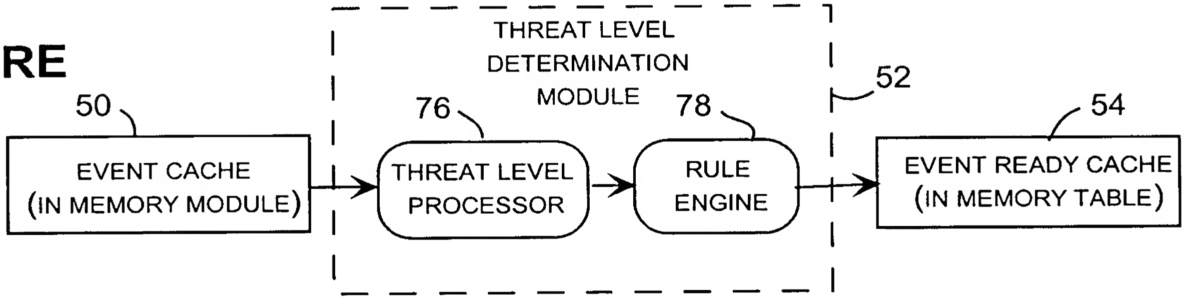

50
EVENT CACHE (IN MEMORY MODULE)
THREAT LEVEL DETERMINATION MODULE
52
76
THREAT LEVEL PROCESSOR
78
RULE ENGINE
54
EVENT READY CACHE (IN MEMORY TABLE)

FIGURE 9

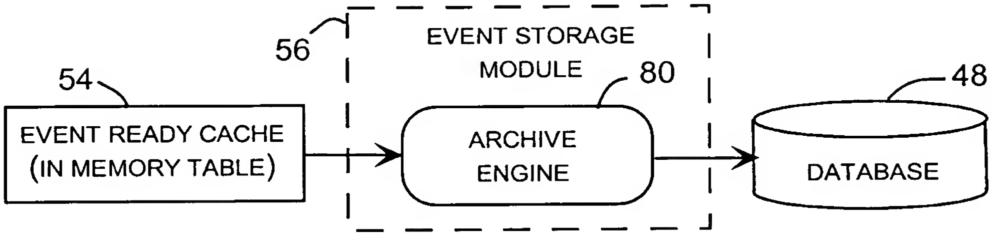


FIGURE 10

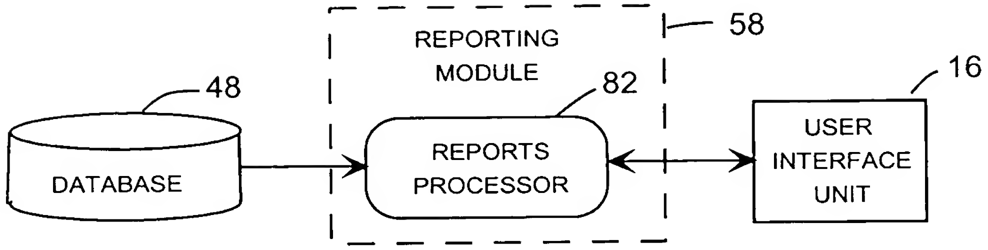


FIGURE 11

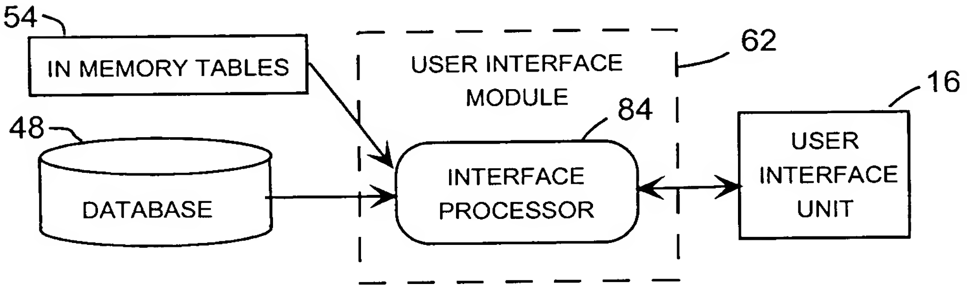
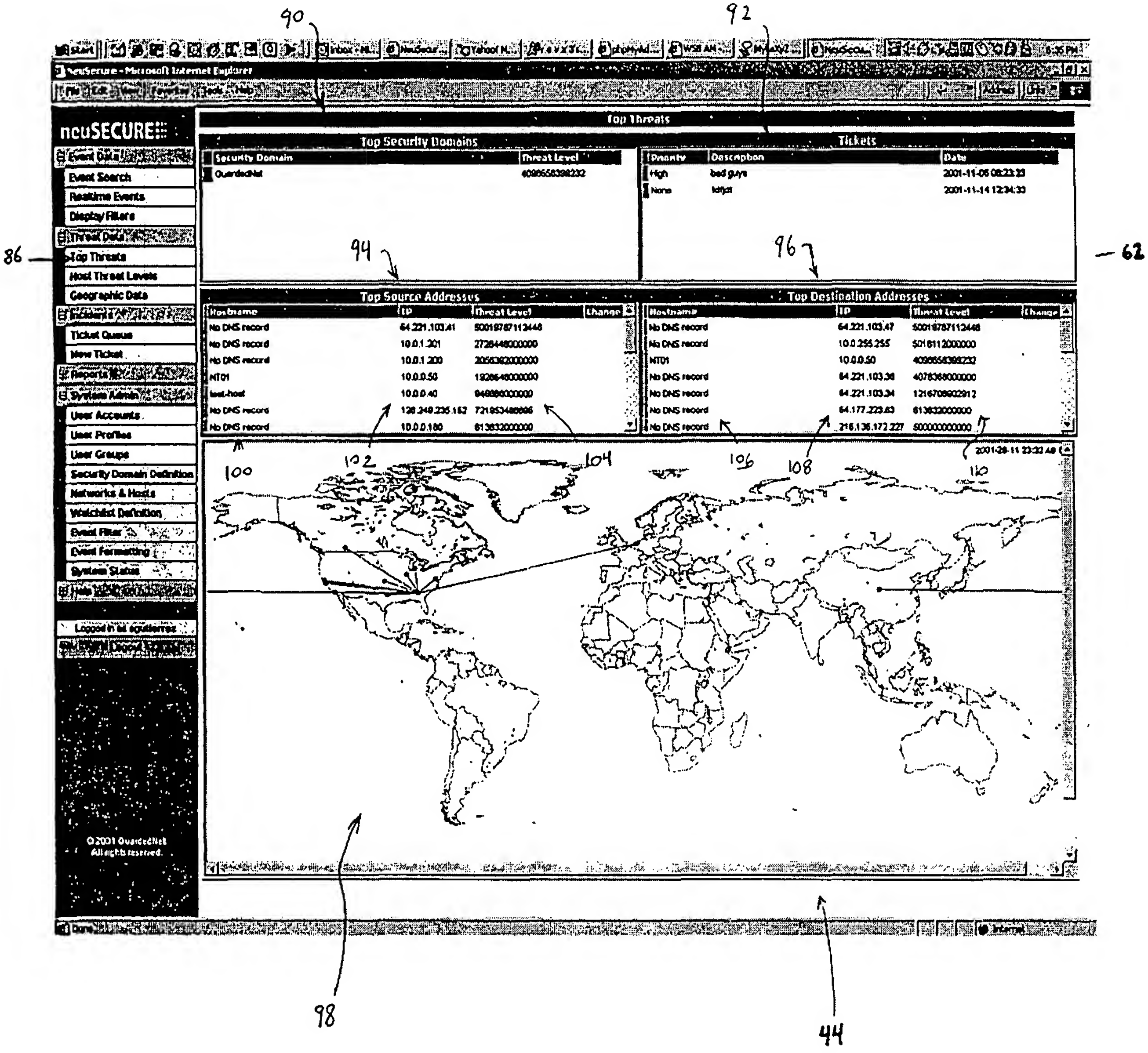


FIGURE 12



Top Threats

Top Security Domains

Security Domain	Threat Level
GuardedNet	4096656398232

Tickets

Priority	Description	Date
High	bad guys	2001-11-05 08:23:23
None	tdfjdf	2001-11-14 12:34:33

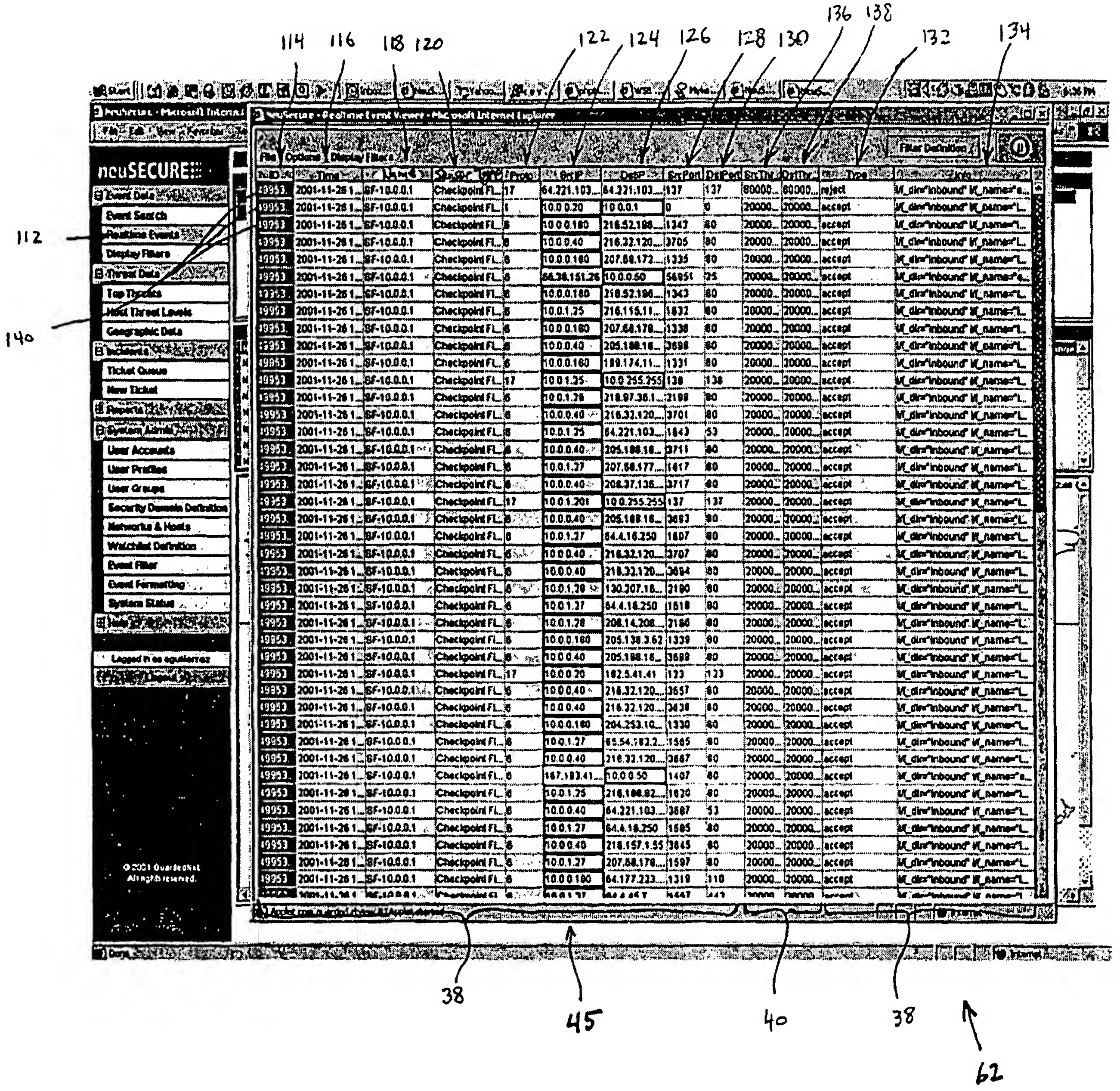
Top Source Addresses

Hostname	IP	Threat Level	Change
No DNS record	64.221.103.41	50019787112448	
No DNS record	10.0.1.201	2728448000000	
No DNS record	10.0.1.200	2056382000000	
NT01	10.0.0.50	1928648000000	
test-host	10.0.0.40	948886000000	
No DNS record	128.249.235.162	721853488886	
No DNS record	10.0.0.180	613832000000	

Top Destination Addresses

Hostname	IP	Threat Level	Change
No DNS record	64.221.103.47	50018787112448	
No DNS record	10.0.255.255	5018112000000	
NT01	10.0.0.50	4096656398232	
No DNS record	64.221.103.36	4078368000000	
No DNS record	64.221.103.34	1216708902912	
No DNS record	64.177.223.83	613632000000	
No DNS record	216.136.172.227	500000000000	

FIGURE 13



NID	Time	Name	[illegible]	Proto	SrcIP	DestP	SrcPort	DstPort	SrcThr	DstThr	Type	Info
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	17	64.221.103...	64.221.103...	137	137	80000...	80000...	reject	M_dir="inbound" M_name="e...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	1	10.0.0.20	10.0.0.1	0	0	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	216.52.186...	1342	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3705	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	207.68.172...	1335	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	66.38.151.26	10.0.0.50	56951	25	20000...	20000...	accept	M_dir="inbound" M_name="e...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	216.52.186...	1343	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.25	216.115.11...	1632	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	207.68.178...	1338	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	205.188.16...	3698	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	189.174.11...	1331	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	17	10.0.1.25	10.0.255.255	138	138	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.28	218.97.36.1...	2198	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3701	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.25	64.221.103...	1643	53	20000...	10000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	205.188.16...	3711	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	207.68.177...	1617	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	208.37.136...	3717	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	17	10.0.1.201	10.0.255.255	137	137	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	205.188.16...	3693	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	64.4.16.250	1607	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3707	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3694	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.28	130.207.16...	2190	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	64.4.16.250	1618	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.28	208.14.208...	2186	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	205.138.3.62	1339	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	205.188.16...	3688	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	17	10.0.0.20	192.5.41.41	123	123	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3657	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3638	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	204.253.10...	1330	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	65.54.182.2...	1565	80	20000...	20000...	accept	M_dir="inbound" M_name="1...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.32.120...	3687	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	167.183.41...	10.0.0.50	1407	80	20000...	20000...	accept	M_dir="inbound" M_name="e...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.25	216.188.82...	1620	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	64.221.103...	3687	53	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	64.4.16.250	1685	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.40	216.157.1.55	3845	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953.	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.1.27	207.68.178...	1597	80	20000...	20000...	accept	M_dir="inbound" M_name="L...
49953	2001-11-26 1...	SF-10.0.0.1	Checkpoint FL...	6	10.0.0.180	64.177.223...	1319	110	20000...	20000...	accept	M_dir="inbound" M_name="L...
[illegible]	2001-11-26 1	SF-10.0.0.1	Checkpoint FL	6	10.0.1.27	64.4.45.7	[illegible]	443	20000	20000	accept	M_dir="inbound" M_name="[illegible]

FIGURE 14

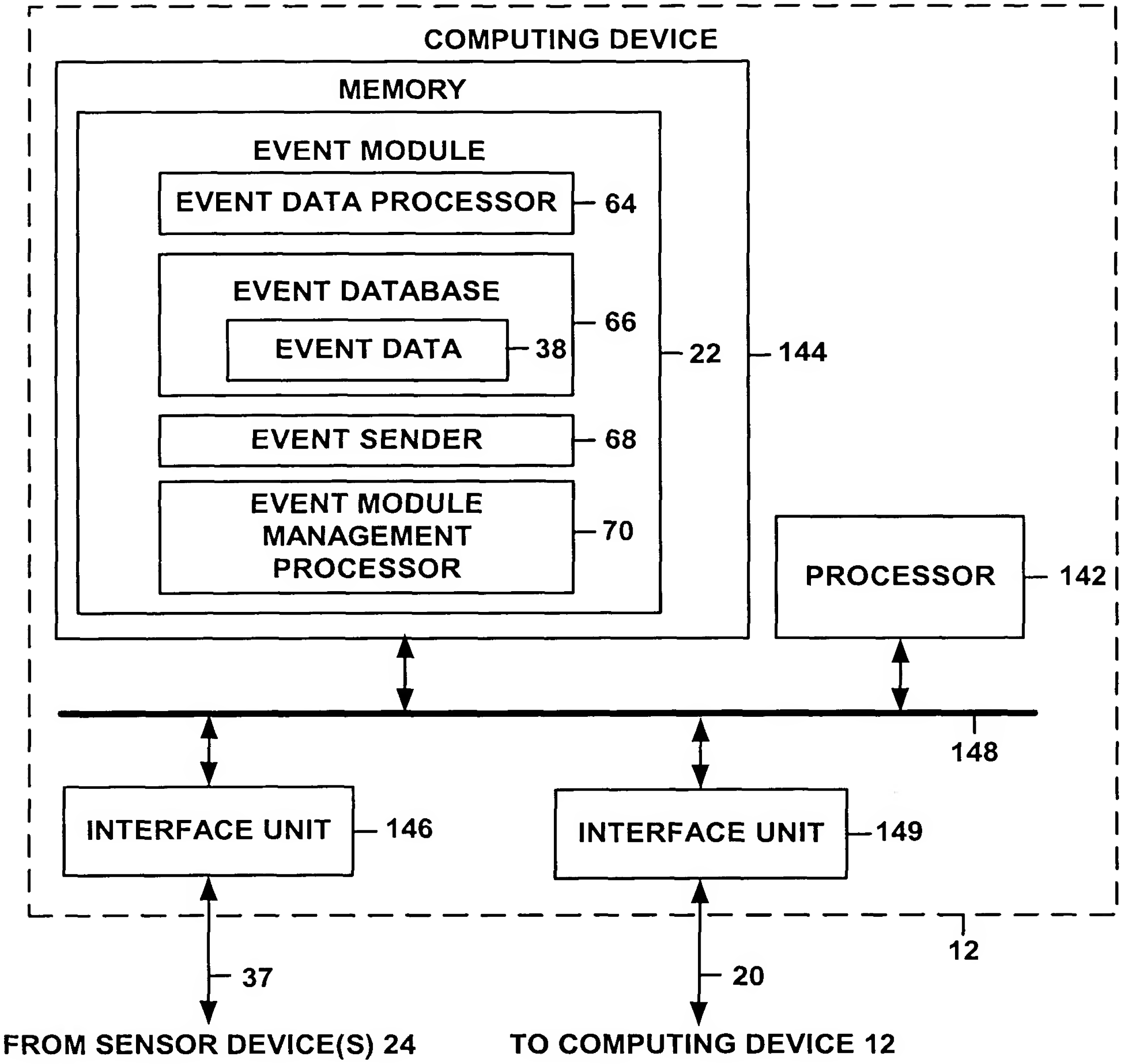
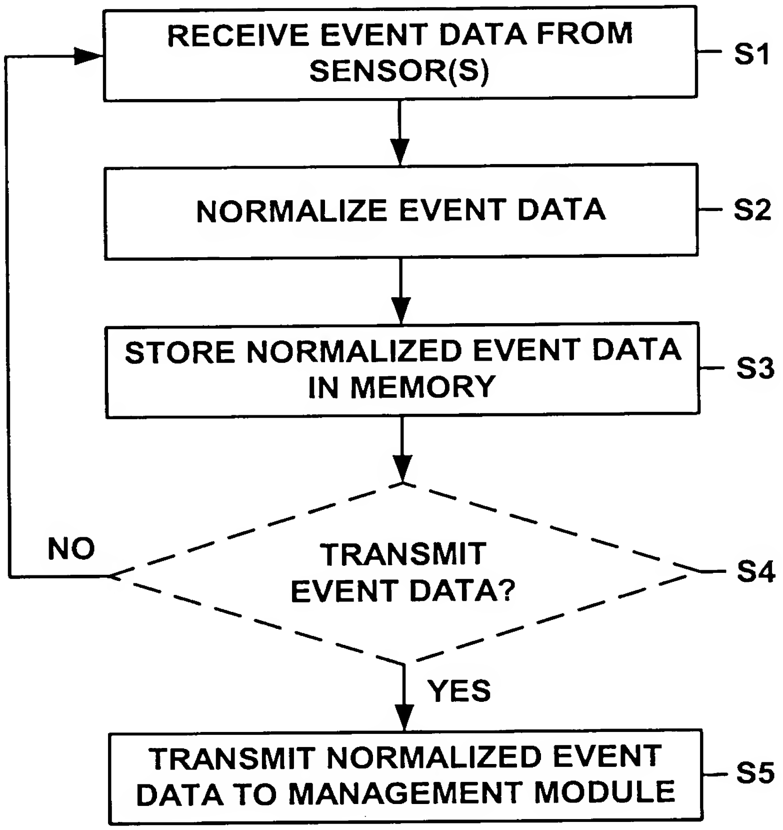

COMPUTING DEVICE
MEMORY
EVENT MODULE
EVENT DATA PROCESSOR
64
EVENT DATABASE
66
EVENT DATA
38
22
144
EVENT SENDER
68
EVENT MODULE MANAGEMENT PROCESSOR
70
PROCESSOR
142
148
INTERFACE UNIT
146
INTERFACE UNIT
149
12
37
20
FROM SENSOR DEVICE(S) 24
TO COMPUTING DEVICE 12

FIGURE 15

PROCESSING OF EVENT DATA BY EVENT MODULE



RECEIVE EVENT DATA FROM SENSOR(S)
S1
NORMALIZE EVENT DATA
S2
STORE NORMALIZED EVENT DATA IN MEMORY
S3
NO
TRANSMIT EVENT DATA?
S4
YES
TRANSMIT NORMALIZED EVENT DATA TO MANAGEMENT MODULE
S5

FIGURE 16

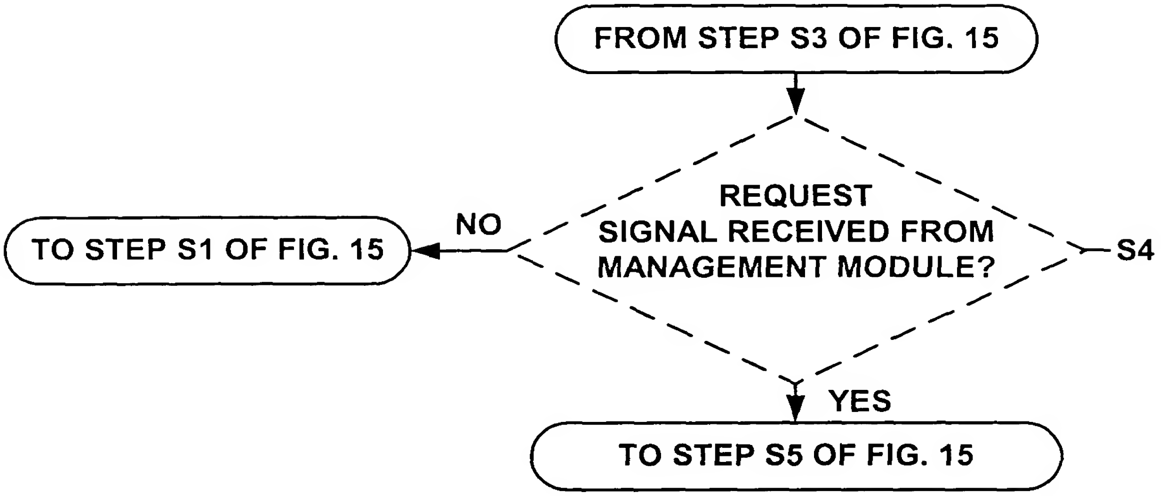


FIGURE 17

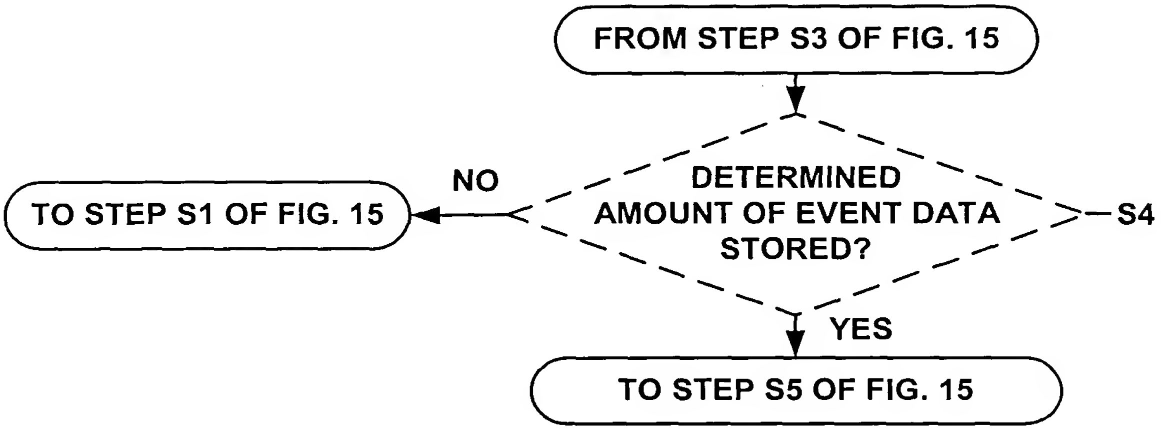


FIGURE 18

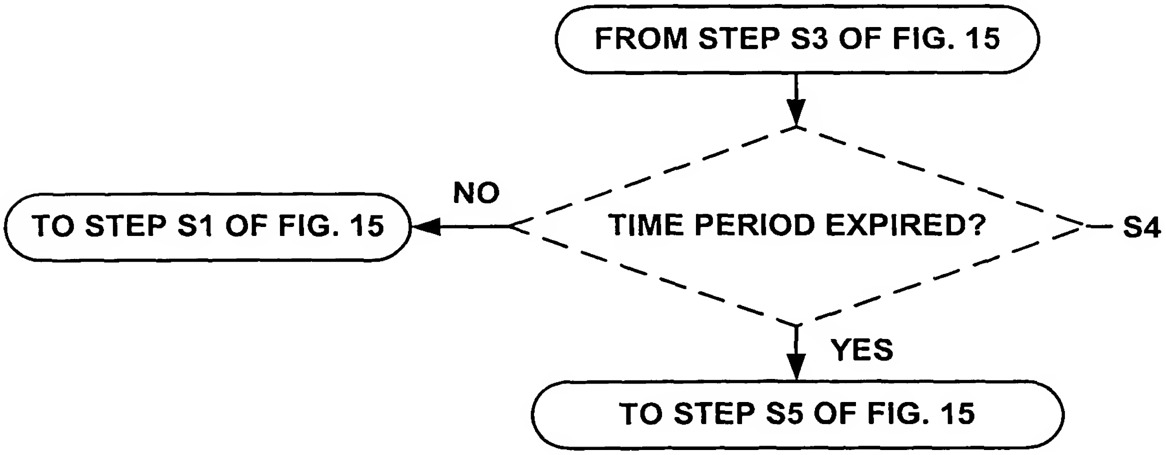


FIGURE 19

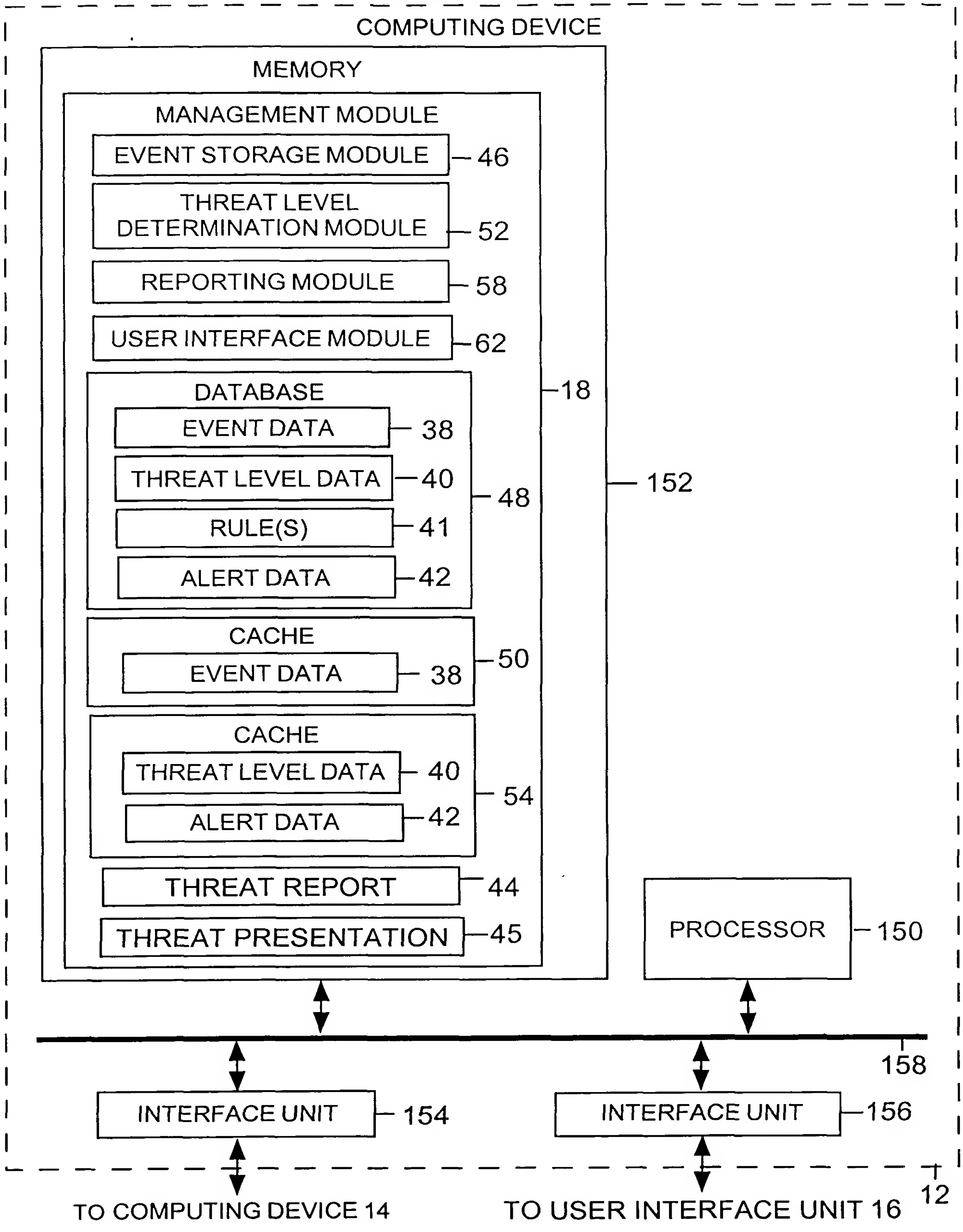

COMPUTING DEVICE
MEMORY
MANAGEMENT MODULE
EVENT STORAGE MODULE
46
THREAT LEVEL DETERMINATION MODULE
52
REPORTING MODULE
58
USER INTERFACE MODULE
62
DATABASE
EVENT DATA
38
THREAT LEVEL DATA
40
RULE(S)
41
ALERT DATA
42
48
18
152
CACHE
EVENT DATA
38
50
CACHE
THREAT LEVEL DATA
40
ALERT DATA
42
54
THREAT REPORT
44
THREAT PRESENTATION
45
PROCESSOR
150
158
INTERFACE UNIT
154
INTERFACE UNIT
156
12
TO COMPUTING DEVICE 14
TO USER INTERFACE UNIT 16

FIGURE 20

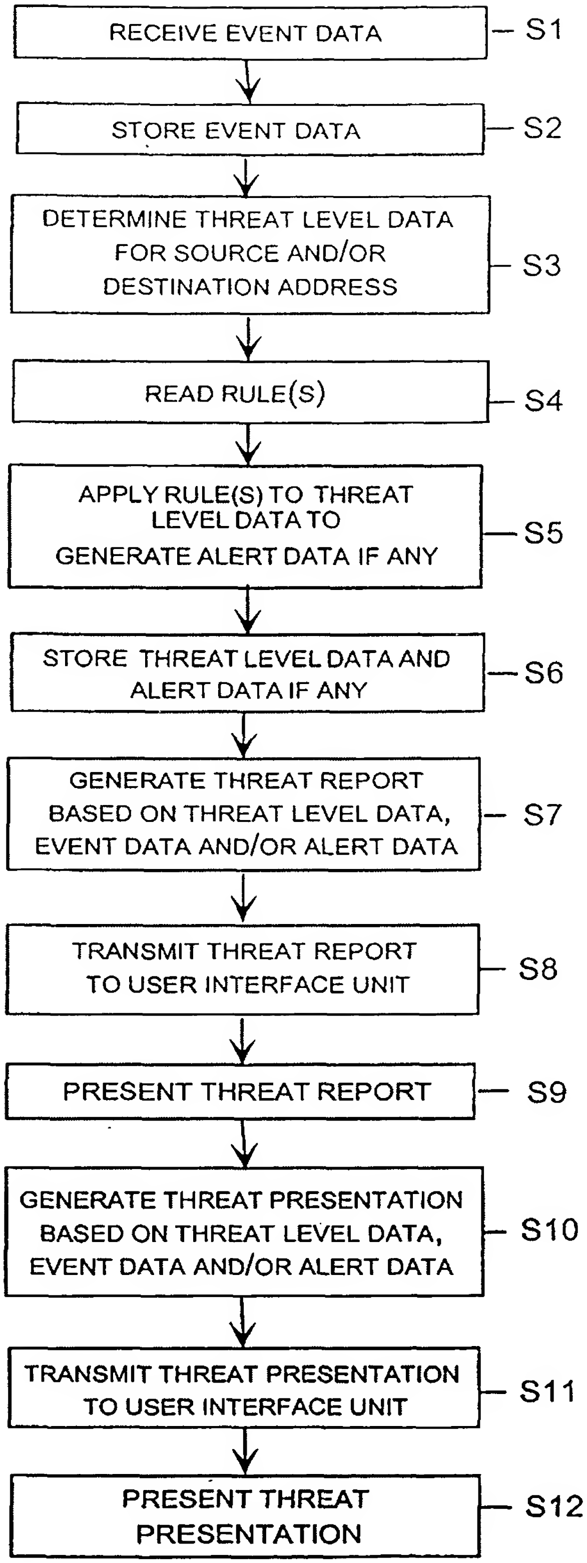

RECEIVE EVENT DATA
S1
STORE EVENT DATA
S2
DETERMINE THREAT LEVEL DATA FOR SOURCE AND/OR DESTINATION ADDRESS
S3
READ RULE(S)
S4
APPLY RULE(S) TO THREAT LEVEL DATA TO GENERATE ALERT DATA IF ANY
S5
STORE THREAT LEVEL DATA AND ALERT DATA IF ANY
S6
GENERATE THREAT REPORT BASED ON THREAT LEVEL DATA, EVENT DATA AND/OR ALERT DATA
S7
TRANSMIT THREAT REPORT TO USER INTERFACE UNIT
S8
PRESENT THREAT REPORT
S9
GENERATE THREAT PRESENTATION BASED ON THREAT LEVEL DATA, EVENT DATA AND/OR ALERT DATA
S10
TRANSMIT THREAT PRESENTATION TO USER INTERFACE UNIT
S11
PRESENT THREAT PRESENTATION
S12

FIGURE 21

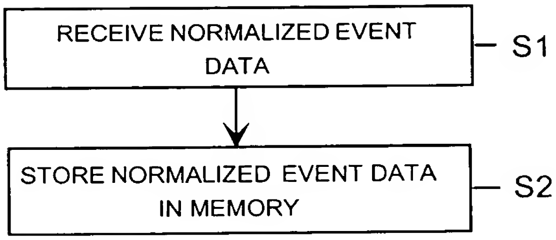

RECEIVE NORMALIZED EVENT DATA
S1
STORE NORMALIZED EVENT DATA IN MEMORY
S2

FIGURE 22

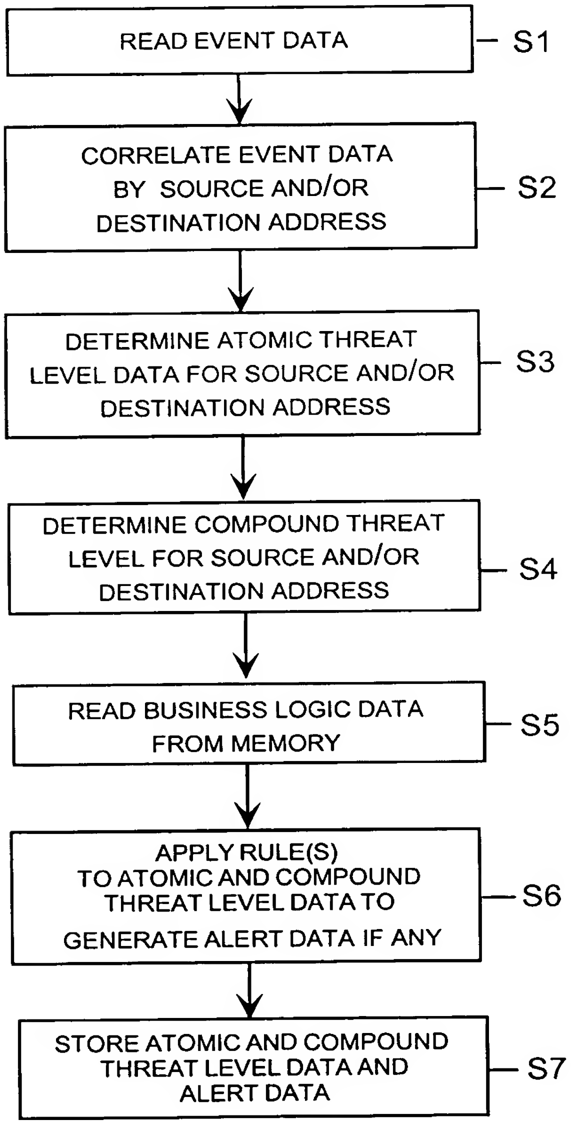

READ EVENT DATA
S1
CORRELATE EVENT DATA BY SOURCE AND/OR DESTINATION ADDRESS
S2
DETERMINE ATOMIC THREAT LEVEL DATA FOR SOURCE AND/OR DESTINATION ADDRESS
S3
DETERMINE COMPOUND THREAT LEVEL FOR SOURCE AND/OR DESTINATION ADDRESS
S4
READ BUSINESS LOGIC DATA FROM MEMORY
S5
APPLY RULE(S) TO ATOMIC AND COMPOUND THREAT LEVEL DATA TO GENERATE ALERT DATA IF ANY
S6
STORE ATOMIC AND COMPOUND THREAT LEVEL DATA AND ALERT DATA
S7

FIGURE 23

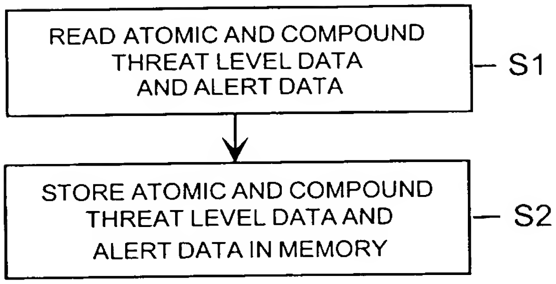

READ ATOMIC AND COMPOUND THREAT LEVEL DATA AND ALERT DATA
S1
STORE ATOMIC AND COMPOUND THREAT LEVEL DATA AND ALERT DATA IN MEMORY
S2

FIGURE 24

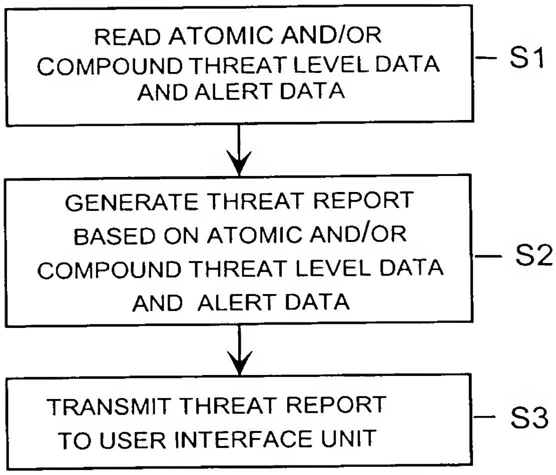

READ ATOMIC AND/OR COMPOUND THREAT LEVEL DATA AND ALERT DATA
S1
GENERATE THREAT REPORT BASED ON ATOMIC AND/OR COMPOUND THREAT LEVEL DATA AND ALERT DATA
S2
TRANSMIT THREAT REPORT TO USER INTERFACE UNIT
S3

FIGURE 25

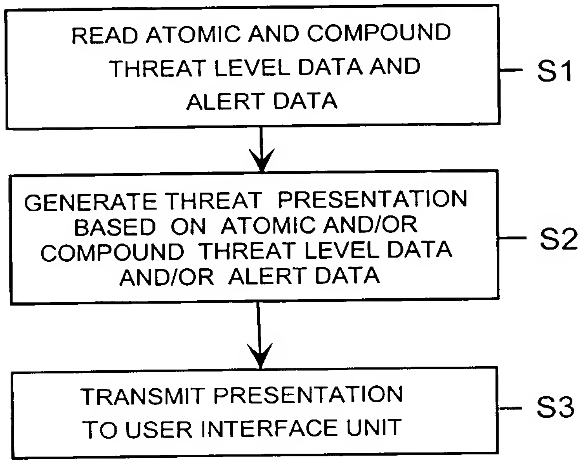
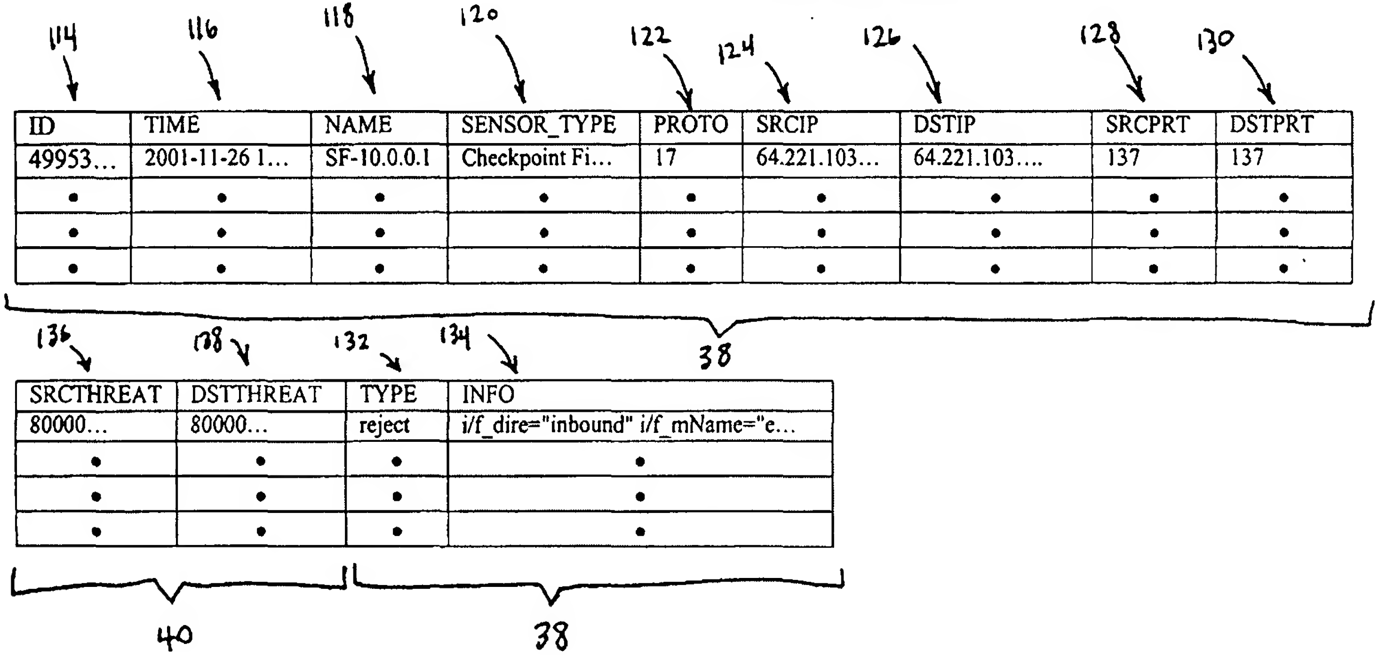

READ ATOMIC AND COMPOUND THREAT LEVEL DATA AND ALERT DATA
S1
GENERATE THREAT PRESENTATION BASED ON ATOMIC AND/OR COMPOUND THREAT LEVEL DATA AND/OR ALERT DATA
S2
TRANSMIT PRESENTATION TO USER INTERFACE UNIT
S3

FIGURE 26


114
116
118
120
122
124
126
128
130
38
136
138
132
134
40
38

ID	TIME	NAME	SENSOR_TYPE	PROTO	SRCIP	DSTIP	SRCPRT	DSTPRT
49953...	2001-11-26 1...	SF-10.0.0.1	Checkpoint Fi...	17	64.221.103...	64.221.103....	137	137
•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•

SRCTHREAT	DSTTHREAT	TYPE	INFO
80000...	80000...	reject	i/f_dire="inbound" i/f_mName="e...
•	•	•	•
•	•	•	•
•	•	•	•

FIGURE 27

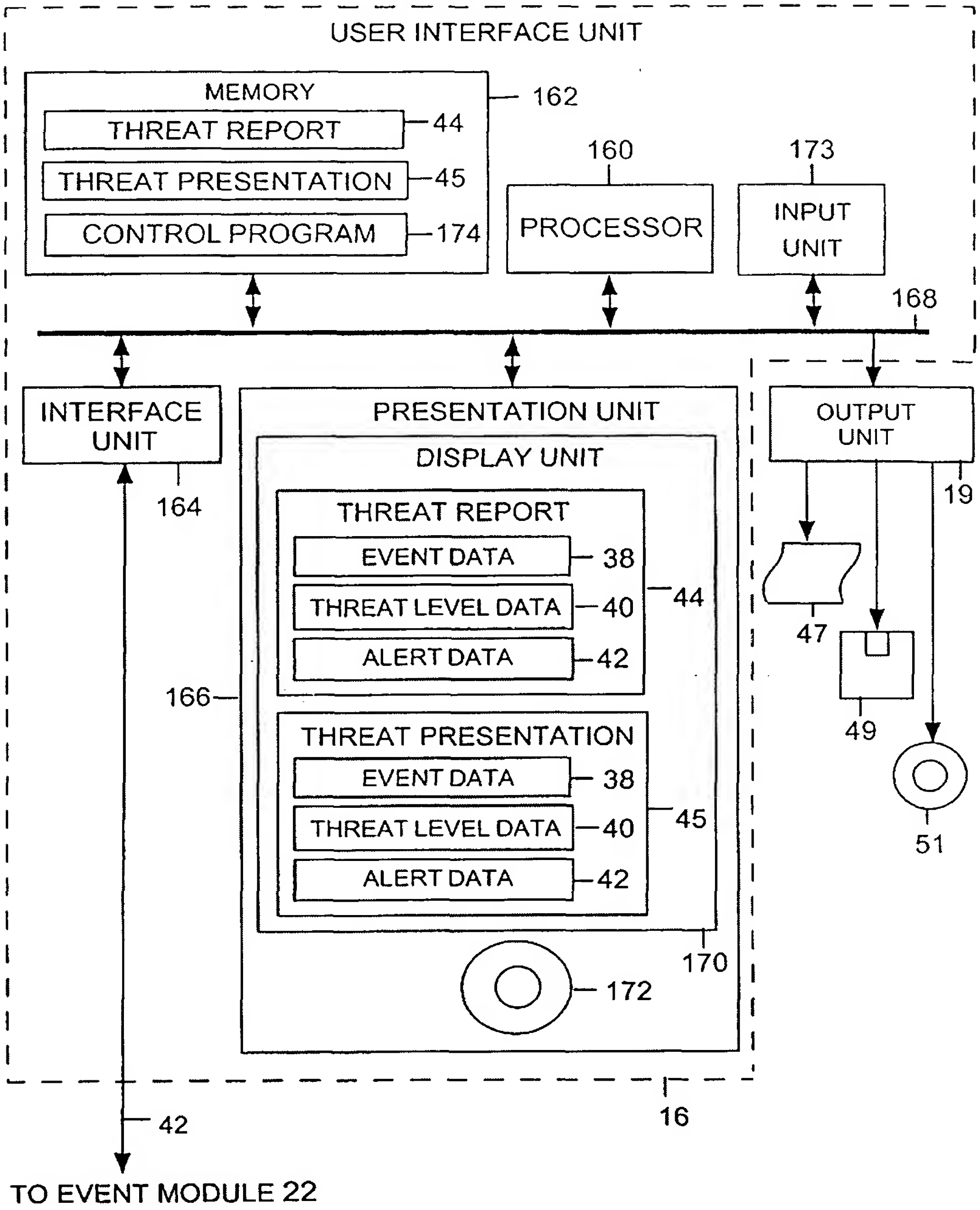

USER INTERFACE UNIT
MEMORY
THREAT REPORT
44
THREAT PRESENTATION
45
CONTROL PROGRAM
174
162
160
PROCESSOR
173
INPUT UNIT
168
INTERFACE UNIT
164
PRESENTATION UNIT
DISPLAY UNIT
THREAT REPORT
EVENT DATA
38
THREAT LEVEL DATA
40
ALERT DATA
42
44
166
THREAT PRESENTATION
EVENT DATA
38
THREAT LEVEL DATA
40
ALERT DATA
42
45
170
172
OUTPUT UNIT
19
47
49
51
16
42
TO EVENT MODULE 22

FIGURE 28

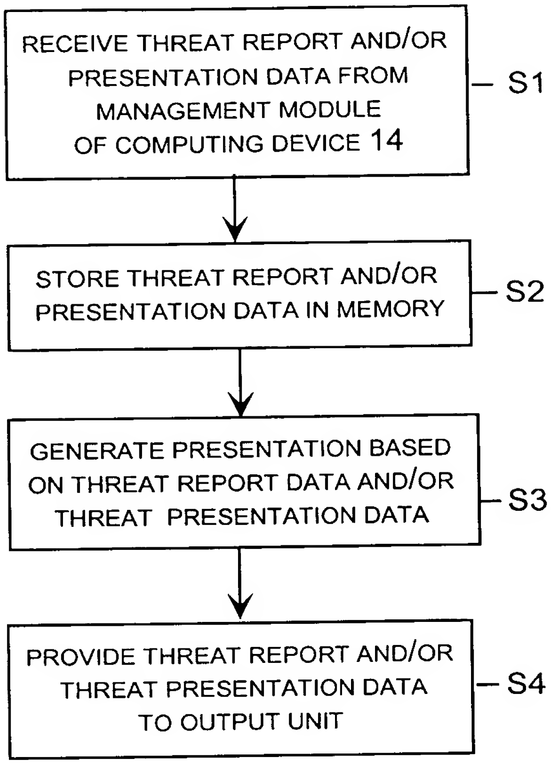

RECEIVE THREAT REPORT AND/OR PRESENTATION DATA FROM MANAGEMENT MODULE OF COMPUTING DEVICE 14
S1
STORE THREAT REPORT AND/OR PRESENTATION DATA IN MEMORY
S2
GENERATE PRESENTATION BASED ON THREAT REPORT DATA AND/OR THREAT PRESENTATION DATA
S3
PROVIDE THREAT REPORT AND/OR THREAT PRESENTATION DATA TO OUTPUT UNIT
S4

FIGURE 29

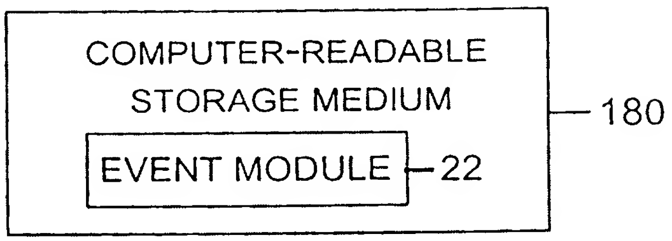


FIGURE 30

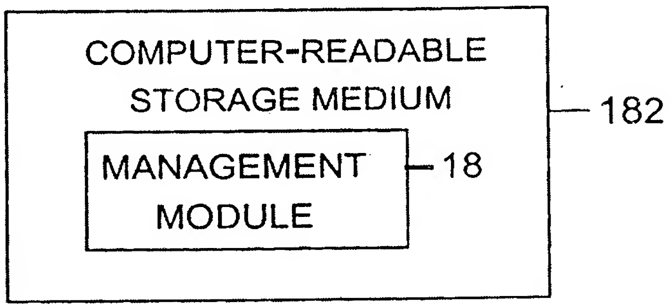
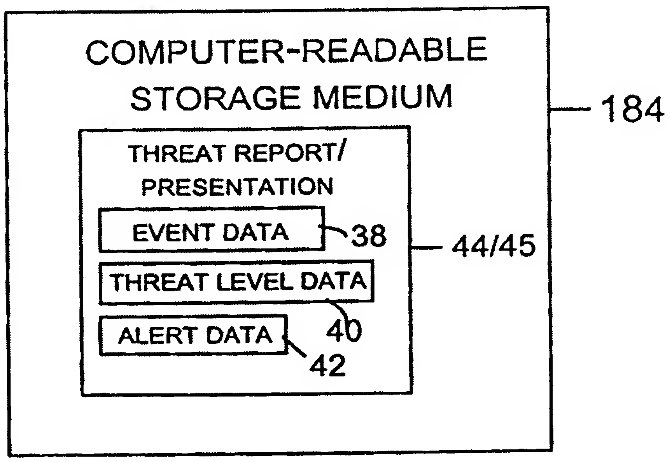
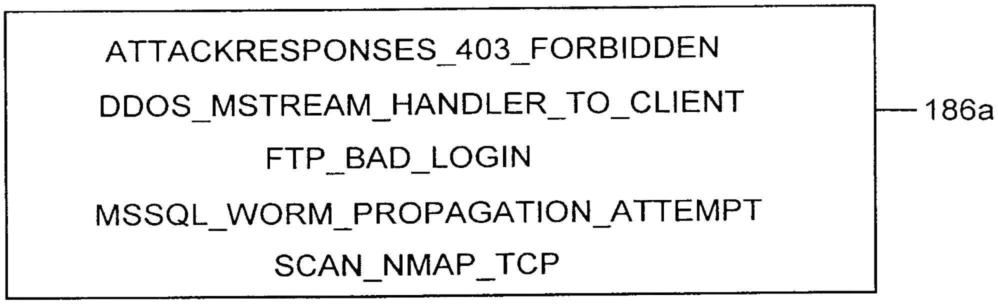


FIGURE 31



EXEMPLARY EVENT TYPES



ATTACKRESPONSES_403_FORBIDDEN

DDOS_MSTREAM_HANDLER_TO_CLIENT

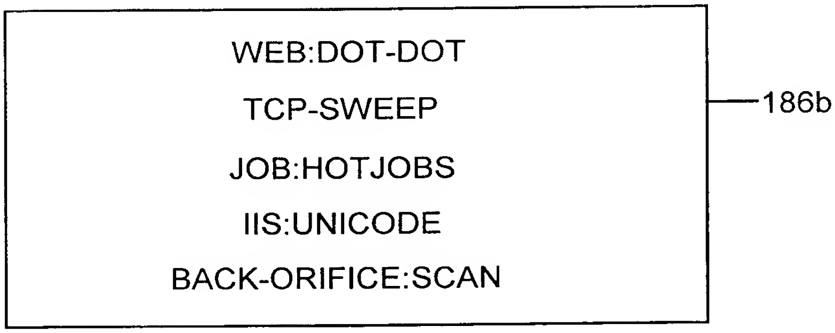
FTP_BAD_LOGIN

MSSQL_WORM_PROPAGATION_ATTEMPT

SCAN_NMAP_TCP

FIGURE 32A

EXEMPLARY EVENT TYPES



WEB:DOT-DOT

TCP-SWEEP

JOB:HOTJOBS

IIS:UNICODE

BACK-ORIFICE:SCAN

FIGURE 32B

CALCULATIONS

190 THREAT

$T(H) = TW[H] * NB\text{-}TW[NB[H]]$

192 SOURCE THREAT

$ST(e) = T(e.src)$

194 DESTINATION THREAT

$DT(e) = T(e.dst)$

196 VULNERABILITY

$DT(e) = T(e.dst)$

198 EVENT VALIDITY

$EV(e) = VALIDITY[e.src][e.type]$

200 EVENT SEVERITY

$ES(e) = PRIORITY[e]$

202 ATOMIC THREAT LEVEL

$AT(e) = EV(e) * V(e) * ST(e) * ES\ (e)$

204 HOST THREAT LEVEL

$$\delta(e,H,t) = \begin{cases} 1 \text{ if } (e.src = H \text{ or } e.dst = H) \\ 0 \text{ otherwise} \end{cases}$$

$$HT(H,t) = \frac{\sum_{i=1}^{N} AT(e_i) * \delta(e_i,H,t)}{\sum_{i=1}^{N} \delta(e_i,H,t)}$$

206 DIFFERENTIAL THREAT LEVEL

$$DTL(H,T_1,T_1) = \frac{HT(H_1,T_1)}{HT(H_1,T_2)} * \frac{T_2}{T_1} \quad \text{WHERE } 0<T_1<T_2$$

FIGURE 33

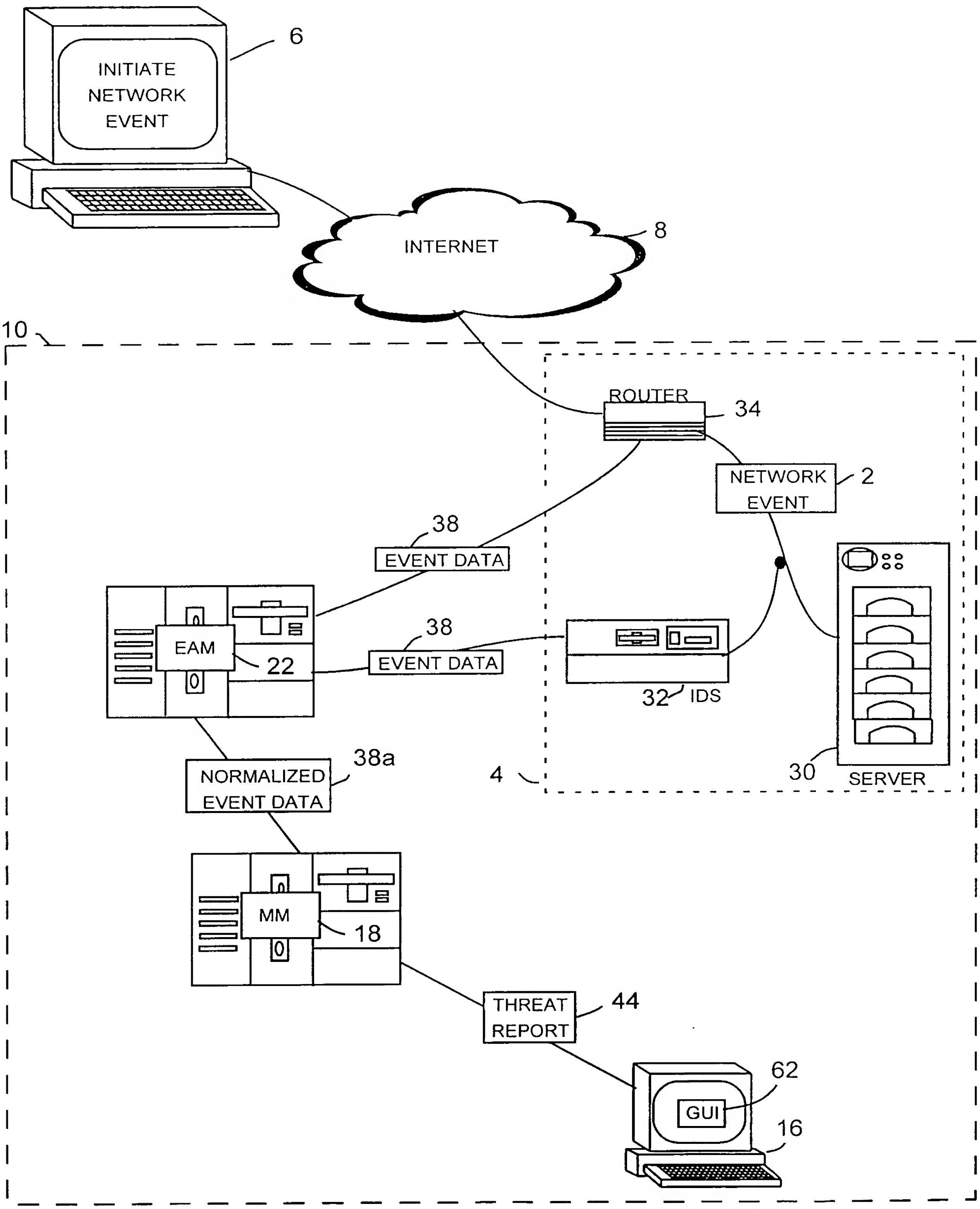

INITIATE
NETWORK
EVENT
6
INTERNET
8
10
ROUTER
34
NETWORK
EVENT
2
38
EVENT DATA
38
EVENT DATA
EAM
22
32
IDS
30
SERVER
4
NORMALIZED
EVENT DATA
38a
MM
18
THREAT
REPORT
44
GUI
62
16

FIGURE 34